CLAIMS

1. A process for storing and recovering security information stored on a first smart card that is used to uniquely access a client computer and secure logins into networks and Web sites, comprising the steps of:

providing a secure server;

creating a password and challenge question;

wherein said password is used to access said server if said first smart card is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a smart card;

retrieving the ID number of said first smart card and other user and system specific information;

storing said first smart card ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; and

providing configuration means for configuring said client to boot only if said first smart card is readable by said client or said first access key is entered.

2. The process of claim 1, wherein an emergency diskette is created and said client can boot using said diskette instead of said first smart card.

3. The process of claim 1, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays said access key to the user if said log in is correct.

4. The process of claim 1, wherein the user enters said first access key into said client; and wherein said client boots in response to said first access key.

5. The process of claim 1, further comprising the steps of:

wherein the user requests that said server issue a second smart card to replace said first smart card;

wherein the user makes said request through said client;

retrieving the ID number from said second smart card;

replacing said first smart card's ID with said second smart card's ID on said server; and

wherein said configuration means configures said client to boot if said second smart card is readable, thereby replacing said first smart card.

6. The process of claim 5, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

7. The process of claim 5, further comprising the step of:

wherein said access key creation means creates a second access key;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

8. The process of claim 5, further comprising the step of:

providing morphing means for recreating the personal computing environment stored on said first smart card onto said second smart card.

9. The process of claim 8, wherein said morphing means transfers the encryption and other rights of said first smart card to said second smart card.

10. The process of claim 1, further comprising the step of:

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

11. The process of claim 1, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first smart card.

12. A process for storing and recovering security information stored on a first smart card that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

retrieving the ID number of said first smart card and other user and system specific information;

storing said first smart card ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; and

providing configuration means for configuring said client to boot only if said first smart card is readable by said client or said first access key is entered.

13. The process of claim 12, further comprising the step of:

creating a password and challenge question; and

wherein said password is used to access said server if said first smart card is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a smart card.

14. The process of claim 12, wherein an emergency diskette is created and said client can boot using said diskette instead of said first smart card.

15. The process of claim 13, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays said access key to the user if said log in is correct.

16. The process of claim 12, wherein the user enters said first access key into said client; and wherein said client boots in response to said first access key.

17. The process of claim 12, further comprising the steps of:

wherein the user requests that said server issue a second smart card to replace said first smart card;

wherein the user makes said request through said client;

retrieving the ID number from said second smart card;

replacing said first smart card's ID with said second smart card's ID on said server; and

wherein said configuration means configures said client to boot if said second smart card is readable, thereby replacing said first smart card.

18. The process of claim 17, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

19. The process of claim 17, further comprising the step of:

wherein said access key creation means creates a second access key;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

20. The process of claim 17, further comprising the step of:

providing morphing means for recreating the personal computing environment stored on said first smart card onto said second smart card.

21. The process of claim 20, wherein said morphing means transfers the encryption and other rights of said first smart card to said second smart card.

22. The process of claim 12, further comprising the step of:

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

23. The process of claim 12, further comprising the step of:

providing automatic login means on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first smart card.

24. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for storing and recovering security information stored on a first smart card that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

creating a password and challenge question;

wherein said password is used to access said server if said first smart card is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a smart card;

retrieving the ID number of said first smart card and other user and system specific information;

storing said first smart card ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; and

providing configuration means for configuring said client to boot only if said first smart card is readable by said client or said first access key is entered.

25. The method of claim 24, wherein an emergency diskette is created and said client can boot using said diskette instead of said first smart card.

26. The method of claim 24, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays said access key to the user if said log in is correct.

27. The method of claim 24, wherein the user enters said first access key into said client; and wherein said client boots in response to said first access key.

28. The method of claim 24, further comprising the steps of:

wherein the user requests that said server issue a second smart card to replace said first smart card;

wherein the user makes said request through said client;

retrieving the ID number from said second smart card;

replacing said first smart card's ID with said second smart card's ID on said server; and

wherein said configuration means configures said client to boot if said second smart card is readable, thereby replacing said first smart card.

29. The method of claim 28, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

30. The method of claim 28, further comprising the step of:

wherein said access key creation means creates a second access key;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

31. The method of claim 28, further comprising the step of:

providing morphing means for recreating the personal computing environment stored on said first smart card onto said second smart card.

32. The method of claim 31, wherein said morphing means transfers the encryption and other rights of said first smart card to said second smart card.

33. The method of claim 24, further comprising the step of:

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

34. The method of claim 24, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first smart card.

35. A program storage medium readable by a computer, tangibly embodying a program of instructions executable by the computer to perform method steps for storing and recovering security information stored on a first smart card that is used to uniquely access a client computer, comprising the steps of:

providing a secure server;

retrieving the ID number of said first smart card and other user and system specific information;

storing said first smart card ID and said other user and system specific information on said server;

providing access key creation means on said server for creating a first access key;

storing said first access key on said server; and

providing configuration means for configuring said client to boot only if said first smart card is readable by said client or said first access key is entered.

36. The method of claim 35, further comprising the step of:

creating a password and challenge question; and

wherein said password is used to access said server if said first smart card is lost and said challenge question is used to confirm the user's identity when challenged while accessing said server without a smart card.

37. The method of claim 35, wherein an emergency diskette is created and said client can boot using said diskette instead of said first smart card.

38. The method of claim 36, wherein the user accesses said server through another computer; wherein said server requires the user to log in; and wherein said server displays said access key to the user if said log in is correct.

39. The method of claim 35, wherein the user enters said first access key into said client; and wherein said client boots in response to said first access key.

40. The method of claim 35, further comprising the steps of:

wherein the user requests that said server issue a second smart card to replace said first smart card;

wherein the user makes said request through said client;

retrieving the ID number from said second smart card;

replacing said first smart card's ID with said second smart card's ID on said server; and

wherein said configuration means configures said client to boot if said second smart card is readable, thereby replacing said first smart card.

41. The method of claim 40, wherein said server requires the user to enter the proper user and/or other system specific information to validate said request.

42. The method of claim 40, further comprising the step of:

wherein said access key creation means creates a second access key;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

43. The method of claim 40, further comprising the step of:

providing morphing means for recreating the personal computing environment stored on said first smart card onto said second smart card.

44. The method of claim 43, wherein said morphing means transfers the encryption and other rights of said first smart card to said second smart card.

45. The method of claim 35, further comprising the step of:

wherein said access key creation means creates a second access key upon request by the user;

replacing said first access key with said second access key on said server; and

wherein said configuration means configures said client to boot if said second access key is entered, thereby replacing said first access key.

46. The method of claim 35, further comprising the step of:

providing automatic login means resident on said client for logging onto networks and/or Web sites, without the user's intervention, using the user's information stored on said first smart card.